corresponding to each of said plurality of data elements to descramble each of said plurality of data elements.

REMARKS

The Examiner's careful consideration of the application is sincerely appreciated. In light of the above amendments and following remarks, reconsideration and allowance of this application are requested.

At paragraph 3 of the outstanding Office Action, the Examiner has rejected claims 4-7 under 35 U.S.C. §112, first paragraph, complaining that while encryption of a multiplexed transport stream packet, and encrypting components of a transport stream with keys that correspond to the component, there is no support for the two encryptions being performed jointly. Applicants have amended claims 4-7 to recite that it is the data elements that are scrambled using a scramble key corresponding to the data element. This amendment makes it clear that claims 4-7 further describe the data element in claim 1. Applicants request that the rejection of claims 4-7 under 35 U.S.C. §112 be withdrawn.

At paragraph 5 of the outstanding Office Action of November 18, 2002, the Examiner rejected claims 1, 3-7 and 120 and 121 are rejected under 35 U.S.C. 102(e) as being anticipated by Kurihara (6,069,956). This rejection is respectfully traversed.

As is set forth in amended independent claims 1 and 120, a subscriber authorization system generates a different scramble key for each data element contained in a transmitted transport data stream, each data element comprising at least a portion of a data program to be output at a receiving device. Thus, as is claimed, different scramble keys are generated and assigned, respectively, to different portions of programs, each including video

data, main audio data, sub-audio data, and private data, for example. Each of these data elements comprises a group of data that form at least a portion of a program to be reproduced together as a program. Thus, the scrambling, and therefore different scrambling keys are applied to data elements that are each intended to comprise at least a portion of an audio/video program.

Applicants submit that the Examiner's argument in paragraph 2 of the outstanding Office Action that the scrambling key is a first component and that any of the other data such as video, audio, or sub audio is a second does not teach the claimed invention. Because the scrambling key does not comprise a portion of a data program to be output, it would not meet the elements of the amended independent claims. Applicants submit that these data elements are described in the specification as comprising at least a portion of an audio/video program, and therefore not new mater, (see page 14, lines 4-20, for example). This is only possible because the data elements are scrambled prior to being multiplexed. To optimize security, the subscriber authorization system updates all of these scramble keys. As is further evidence that a scramble key is not a claimed data element, Applicants refer to claim 6 where a scramble key is enciphered separately from the data elements, and then multiplexed with the data elements. Only if the scramble key is different from a data element, would it receive separate treatment in a claim.

The Examiner has stated that "Element 21 of figure 2 anticipates the first part of the first clause of claim 1...[and] Lines 63-64 of column 7 anticipate periodic scramble key updates...[and] Lines 19-26 of column 16 anticipate scramble means." The Examiner also stated "With respect to claim 120, lines 28-29 of column 10 show an enciphered scramble key." However, Applicants submit that while Kurihara may show the information of the time-division frame and the scramble keys being updated, a single scramble key is applied to the audio/video

data element (see col. 9, lines 1-5 and Figs. 12, 13). Therefore, the reference fails to disclose that each data element that is scrambled with a different scramble key comprises a portion of a program to be output, and that all of these scramble keys are updated at predetermined intervals.

Therefore, withdrawal of the rejections to claim 1 under 5 U.S.C. §102(e) is respectfully requested. For reasons similar to those described above with regard to claim 1, withdrawal of the rejections to independent claim 120, as amended herein, is respectfully requested. Accordingly, Applicants submit, therefore, that the present application is in condition for allowance. An early notice to this effect is respectfully solicited.

Claims 2-5, and 121 are dependent from one of claims 1 and 120, and, due to such dependency are distinguishable for the same reasons as the independent claims. Therefore, withdrawal of the rejections to claims 2-5 and 121 is respectfully requested.

In light of the above, Applicants' representative traverses the Examiner's rejections and respectfully submits that the references, alone or in combination do not teach or suggest all of the features of the present invention, as claimed. In view of the foregoing amendments and remarks, it is believed that all of the claims now in this application are patentable over the prior art. Early and favorable consideration thereof is solicited. On the basis of the above amendments and remarks, reconsideration and allowance of this application are respectfully requested.

The above statements concerning the disclosures in the cited references represent the present opinion of Applicants' representative and, in the event that the Examiner disagrees, Applicants' representative respectfully requests the Examiner specifically indicate those portions of the respective references providing the basis for a contrary view.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: _____
Gordon Kessler
Registration No. 38,511
Tel. (212) 588-0800

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Claims 1, 4-7 and 120 have been amended as follows:

1. (Three times Amended) A data multiplexing device which multiplexes a plurality of data elements, each comprising at least a portion of a data program to be output at a receiving device, and transmits said multiplexed data elements as a transport data stream, comprising:

scramble key generation means for generating a plurality of scramble keys, one corresponding to each of said plurality of data elements, wherein each of said scramble keys is updated at predetermined intervals; and

scramble means for scrambling said plurality of data elements by using said corresponding one of said scramble keys generated by said scramble key generation means to scramble a corresponding one of each of said plurality of data elements.

4. (Amended) A data multiplexing device according to claim 1, wherein said scramble means scrambles each of said multiplexed [transport stream packets] data elements by using said scramble key corresponding to each of said [transport stream packet] data elements.

5. (Amended) A data multiplexing device according to claim 4, wherein said scramble means searches for each scramble key for scrambling each of said [transport stream packet] data elements by using a correspondence table which shows packet identification codes for each of said [transport stream packets] data elements and their corresponding scramble keys.

6. (Amended) A data multiplexing device according to claim 4, wherein said data multiplexing device comprises a first encryption means for enciphering said scramble key with a work key and multiplexes said enciphered scramble key with each of said [transport stream packet] data elements to transmit it.

7. (Amended) A data multiplexing device according to claim 6, wherein said data multiplexing device comprises a second encryption means for enciphering said work key with a master key and multiplexes said enciphered work key with each of said [transport stream packet] data elements to transmit it.

120. (Three times Amended) A data reception device for receiving a transport data stream including multiplexed data obtained by multiplexing a plurality of data elements, each comprising at least a portion of a data program to be output at a receiving device, said data reception device comprising:

scramble key extract means for extracting from said multiplexed data a plurality of enciphered scramble keys, one corresponding to each data element, wherein each of said enciphered scramble keys is updated at predetermined intervals; and

descramble means for descrambling said transport data stream including said plurality of data elements by using a scramble key extracted by said scramble key extract means corresponding to each of said plurality of data elements to descramble each of said plurality of data elements.